WE CLAIM:

1. A method for secure communication between first and second domains comprising:

identifying a sender of an encrypted data transmission received from a logical unit using a personal identifier associated with the data transmission;

determining whether the sender is authorized to perform the data transmission;

decrypting the data transmission if it is determined that the sender is authorized to perform the data transmission; and

transmitting the decrypted data to server

2. The method of claim 1 wherein the personal identifier is one of a biometric and a digital signature.

3. The method of claim 1 wherein determining whether the sender is authorized to perform the data transmission includes checking an access control list to determine the sender's privilege level.

4. The method of claim 1 further comprising preventing the data transmission from reaching the application server if it is determined that the sender is not authorized to perform the data transmission function.

5. The method of claim 1 further comprising enhancing data prior to sending the data transmission.

6. An article of manufacture comprising:

a computer usable medium having computer readable program code embodied therein for securely transmitting data from a trusted domain to an untrusted domain comprising:

first computer readable program code for causing a first logical unit to identify a sender of an enhanced data transmission received from a second logical unit;

computer readable program code for determining whether the sender is authorized to perform the data transmission; and

computer readable program code for causing the first logical unit to de-enhance the data; and

computer readable program code for causing the first logical unit to send the data to a third logical unit.

7. The article of manufacture of claim 6 wherein the data in the enhanced data is encrypted.

8. The article of manufacture of claim 6 wherein enhanced data includes biometrically secured data.

9. The article of manufacture of claim 6 further comprising computer readable program code for causing the first logical unit to determine a privilege level of the sender by searching an access control list that contains the sender's privilege level.

10. The article of manufacture of claim 6 further comprising program code for preventing the data from reaching the third logical unit if it is determined that the sender is not authorized to transmit the data.

11. A logical unit programmed to facilitate secure communication between first and second domains comprising:

a processor programmed to receive enhanced data transmitted from a first logical unit and to identify the sender of the enhanced data;

an access control list stored in a memory location including including access rights for the sender;

said processor further being programmed to query said access control list to determine whether the sender has sufficient rights to perform the data transmission, said processor being further programmed to de-enhance the data and to transmit the

data to the second domain when it is determined that the sender has sufficient rights to perform data transmission.

.

12. A logical system for secure communication between first and second domains:

a first logical unit configured to enhance data and to transmit the enhanced data through an outbound proxy across the first secure domain;

a second logical unit configured to receive data from said first logical unit, said second logical unit defining a boundary between the first domain and the second domain, said second logical unit being further configured to identify a sender of the enhanced data, to determine whether the sender has sufficient rights to perform the data transmission, said processor being further configured to de-enhance the data and to transmit the data to a logical unit in the second domain when it is determined that the sender has sufficient rights to perform data transmission.